УДК 62-192:519.713

Е-СЕТЕВОЕ МОДЕЛИРОВАНИЕ НАДЕЖНОСТИ ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНЫХ ТЕХНИЧЕСКИХ СИСТЕМ С ВОССТАНОВЛЕНИЕМ

А.А. Ефремов

Томский политехнический университет
E-mail: alex_yefremov@mail.ru

Показана возможность моделирования процессов отказов-восстановлений последовательно-параллельных технических систем с использованием аппарата Е-сетей. Разработаны сети для различных типов параллельного резервирования. Учтена возможность моделирования надежности восстанавливаемых объектов.

К современным вычислительным системам и сетям связи предъявляются многогранные технические требования. Поэтому, для реализации сложных систем, таких как автоматизированные системы управления, необходимо использовать тысячи различных элементов. Сложность аппаратуры отрицательно сказывается на ее надежности. Проблема повышения надежности настолько сложна, что ее решение требует компьютерного моделирования процессов, протекающих в системе, для того чтобы облегчить работу проектировщиков сложных технических систем.

Среди моделей систем интенсивно развивается аппарат Е-сетей [1], преимуществами которого являются его наглядность, возможность адекватного описания систем с параллельно функционирующими компонентами и приспособленность сетевых моделей для анализа с помощью ЭВМ.

Являясь расширением сетей Петри, Е-сети представляют собой графическое и математическое средство моделирования, применимое к системам самых различных типов. В качестве графического средства они могут использоваться для наглядного представления моделируемой системы подобно блок-схемам и графам. В качестве математического средства Е-сети позволяют составлять уравнения состояния и другие математические соотношения, описывающие динамику систем.

Е-сеть, как и сеть Петри, имеет структуру двудольного ориентированного графа, у которого вершины одного типа образуются позициями, а другого – переходами. Дуги в Е-сетях могут связывать только переход с позицией или позицию с переходом. Входить и выходить из позиции может не более одной дуги.

Существует несколько типов позиций [2]:

- простые (могут содержать не более одной фишки и изображаются кружком);
- очереди (могут содержать произвольное число фишек и изображаются овалами);
- разрешающие (выполняют управляющую функцию, определяющую направление перемещения фишек; изображаются квадратом).

Переходы в Е-сетях (изображаются отрезком прямой линии) могут быть ассоциированы с:

- временной задержкой;
- процедурой преобразования атрибутов фишек, проходящих через переход;
- разрешающей процедурой, если переход имеет входную разрешающую позицию.

Следует отметить, что для усиления выразительных средств Е-сетей разрешающие процедуры, процедуры преобразования атрибутов, сетевых переменных и процедуры вычисления временных задержек могут иметь абсолютно произвольный вид и реализовывать любые вспомогательные вычисления и действия, необходимые пользователю.

Процесс работы Е-сети заключается в перемещении фишек из входных позиций переходов в выходные в результате срабатывания переходов. Для этого на каждом шаге модельного времени определяются переходы, готовые сработать, и при этом выполняются следующие действия для каждого из переходов:

1. проверка активности перехода;
2. выполнение разрешающей процедуры, если таковая имеется у данного перехода;
3. определение длительности активной фазы перехода с помощью процедуры вычисления временной задержки;
4. после завершения активной фазы перехода фишки перемещаются из входных позиций в выходные, и выполняется процедура преобразования атрибутов.

В основе Е-сетевого моделирования лежит, фактически, событийно-управляемое моделирование, что, в совокупности с методами генерации случайных чисел для задания времени срабатывания переходов, дает один из наиболее распространенных способов моделирования. Тот факт, что модель управляется событиями, свидетельствует о том, что состояние системы изменяется только при срабатывании переходов и остается неизменным между срабатываниями. Так как время срабатывания переходов является случайной величиной, то для получения статистически достоверных результатов требуется соответствующее количество запусков модели.

Необходимо также ввести некоторые определения из теории надежности [3, 4].

Надежность компонента – это вероятность того, что он будет выполнять свою функцию в течение определенного промежутка времени при работе в нормальных (или заданных) внешних условиях.

Отказ – событие или нерабочее состояние, при котором компонент или его часть не работает или не может работать, как заранее определено.

Вероятность безотказной работы – вероятность того, что элемент способен выполнять свою функцию в течение определенного промежутка времени при заданных условиях; что при заданных условиях работы в интервале безотказной работы системы отказ не возникнет.

Говорят, что компоненты системы соединены *последовательно*, если для работы системы необходимо, чтобы каждый из них работал, т. е., отказ любого компонента вызывает отказ системы.

Когда надежность последовательной системы не удовлетворяет проектным требованиям и улучшение составных компонентов невозможно (более надежные части не доступны или слишком дороги), становится необходимым действовать на структурном уровне и использовать резервированные конфигурации. Говорят, что конфигурация системы *резервированная (параллельная)*, когда появление отказа компонента не обязательно ведет к отказу системы.

Существует три типа параллельного резервирования [5]:

1. При *горячем резервировании* все *M* компонентов модуля находятся в рабочем состоянии, или «*полностью нагружены*» при использовании. Это означает, что все они стареют одновременно.
2. При *холодном резервировании* используется (нагружен) один компонент, а остальные (*M*–1) компонентов модуля находятся в резерве. Когда используемый компонент отказывает, один из резервных компонентов подключается с помощью механизма переключения.
3. При *недогруженном резервировании* резервные компоненты с течением времени стареют. Это эквивалентно ситуации, когда резерв может рассматриваться как частично нагруженный, в отличие от полностью нагруженного при горячем резервировании и не нагруженного при холодном.

Системы называются *восстанавливаемыми*, если основной и резервные компоненты могут восстанавливаться после отказа.

Рассмотрим E-сеть, построенную для компонента резервированной группы с недогруженным резервированием и восстановлением (рис. 1).

Трем состояниям компонента соответствуют три позиции: *S*1 – компонент находится в резерве, *S*6 – компонент в рабочем состоянии, *S*17 – компонент отказал и восстанавливается. Только три перехода обладают случайной временной задержкой: *T*1 – время до отказа из состояния резерва, *T*5 – время до отказа из рабочего состояния, *T*12 – время до восстановления. Временная задержка остальных переходов равна нулю. В начале моделирования фишка может находиться в позиции *S*6, если компонент является основным, и в позиции *S*1, если он резервный.

Рассмотрим возможные маршруты фишки, предполагая, что первоначально она находится в позиции *S*6 (основной компонент).

По истечении случайного времени t_5, записанного в атрибуте фишки позиции *S*6, компонент отказывает. Фишка проходит маршрут *S*8–*S*12–*S*14–*S*17, компонент становится на восстановление, которое занимает время t_{12}, связанное с переходом *T*12. При переходе через *T*8 на упра-

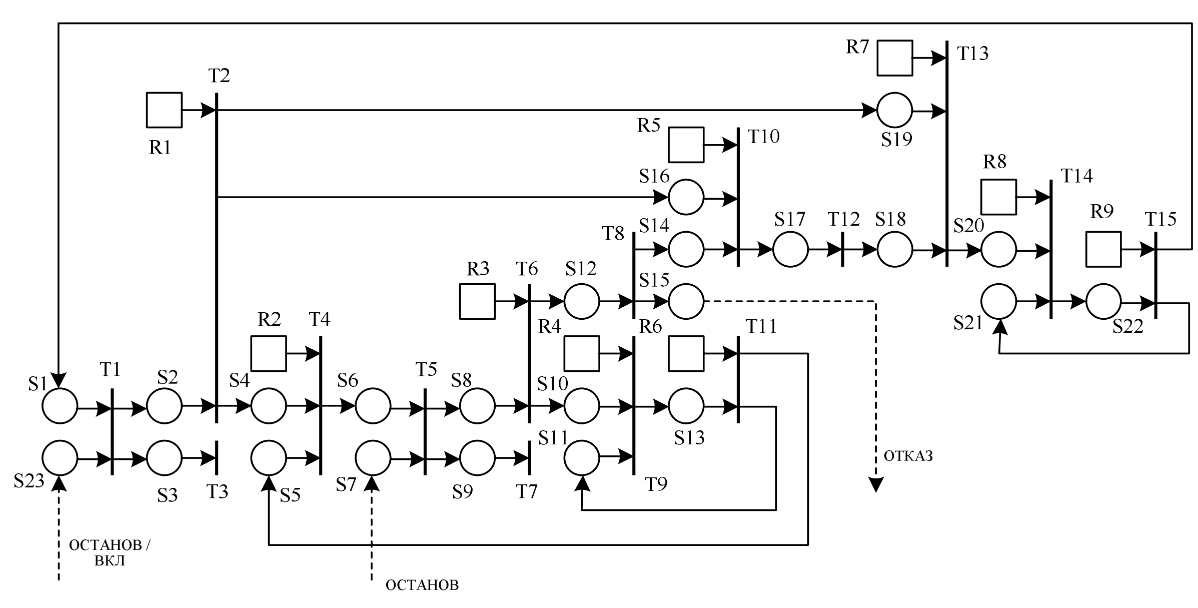


Рис. 1. *E-сеть для компонента параллельной системы (недогруженное резервирование с восстановлением)*

вляющее устройство (УУ) посылается сигнал об отказе компонента. После восстановления фишка проходит маршрут *S*18–*S*20–*S*1 – компонент занимает место в резерве. Находясь в недогруженном резерве, компонент может отказать через случайное время $t_1 >> t_5$. Тогда фишка проследует маршрутом *S*1–*S*2–*S*16–*S*17 и далее (после восстановления) *S*18–*S*20–*S*1 – снова в резерв.

Резервный компонент может также получить от УУ сигнал ВКЛ на подключение в рабочее состояние (фишка в позицию *S*23). Это происходит, если остальные компоненты резервной группы отказали. Тогда нормальная работа перехода *T*1 прерывается, и фишка из *S*1 переходит маршрутом *S*1–*S*2–*S*4–*S*6 в рабочее состояние.

Возможна ситуация, когда работающему компоненту от УУ поступает сигнал ОСТАНОВ, прерывающий моделирование (фишка в позицию *S*7). Это происходит, если система отказала по причине выхода из строя какого-нибудь последовательно соединенного компонента. Тогда в атрибут фишки записывается оставшееся время моделирования, нормальная работа перехода *T*5 прерывается, и фишка следует маршрутом *S*6–*S*8–*S*10 и далее зацикливается в позициях *S*13–*S*11 до тех пор, пока работа системы не восстановится. Тогда фишка вновь занимает позицию *S*6 через *S*13–*S*5, и моделирование продолжается.

Аналогичная ситуация может произойти, когда компонент находится в резерве. Фишка проследует маршрутом *S*2–*S*19–*S*20 и далее цикл в позициях *S*22 – *S*21. При восстановлении работоспособности системы фишка из *S*22 поступает вновь в *S*1 (резерв). Различие между сигналами ВКЛ и ОСТАНОВ для резерва определяется по атрибуту фишки в позиции *S*23.

Если система отказала во время восстановления компонента, то после его восстановления фишка ожидает разрешения (цикл *S*22–*S*21) проследовать в позицию *S*1 (резерв).

Большой размер данной сети объясняется тем, что недогруженное резервирование с восстановлением является наиболее общим и сложным случаем. В случаях горячего и холодного резервирования, а также резервирования без восстановления, сети существенно упрощаются и получаются путем удаления лишних позиций, переходов и связанных с ними дуг (рис. 2–4).

Следует отметить, что Е-сети для горячего резервирования совпадают с сетями для последовательно включенных компонентов.

Важнейшей частью любой последовательно-параллельной системы является управляющее устройство. Именно оно принимает решение о подключении резервных компонентов и об остановке работы системы в целом. В каждом случае Е-сеть для УУ должна строиться отдельно, т. к. необходимо учитывать все возможные комбинации отказов. Приведем пример УУ для системы (рис. 5), состоящей из двух параллельно работающих компонентов *A* и *B* и последовательного компонента *C* (параллельные компоненты в недогруженном резерве, есть возможность восстановления всех трех компонентов).

На вход УУ поступают сигналы об отказах составляющих системы. В случае отказа последовательного компонента *C*, вся система отказывает. Также необходимо остановить работу компонентов *A* и *B*. Поэтому, фишка проходит маршрутом *S*3–*S*4–*S*7, и далее одновременно посылаются сигналы об отказе (*S*22) и останове работы устройств *A* и *B* (*S*10 и *S*11 соответственно). Сигналы об останове компонентов должны прервать как работу резерва, так и работающего устройства, поэтому фишки поступают на

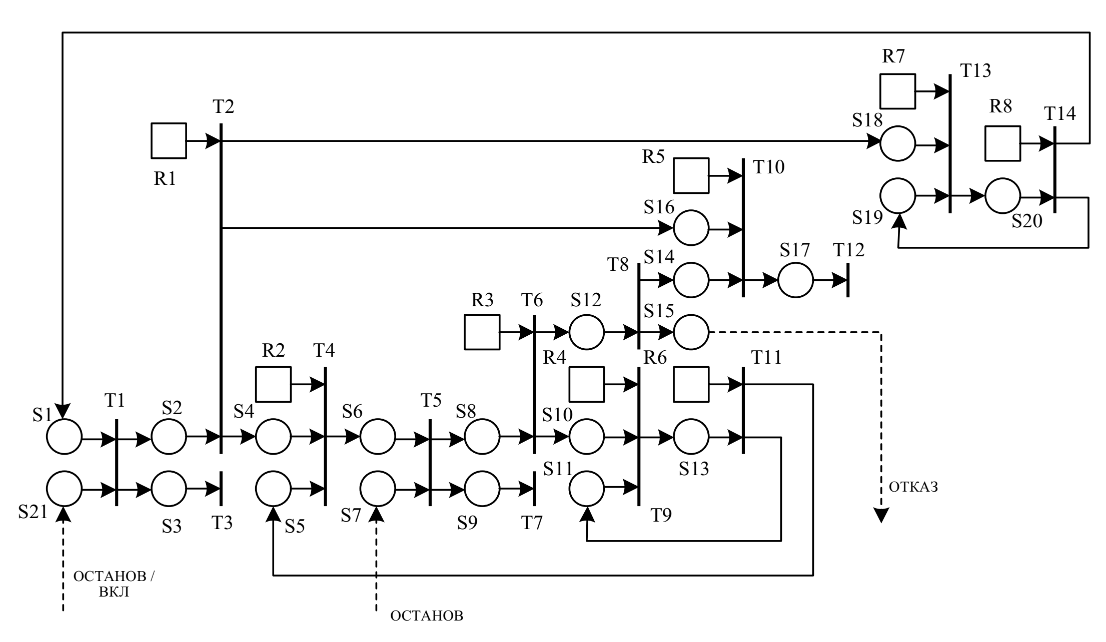


Рис. 2. *Е-сеть для компонента параллельной системы (недогруженное резервирование без восстановления)*

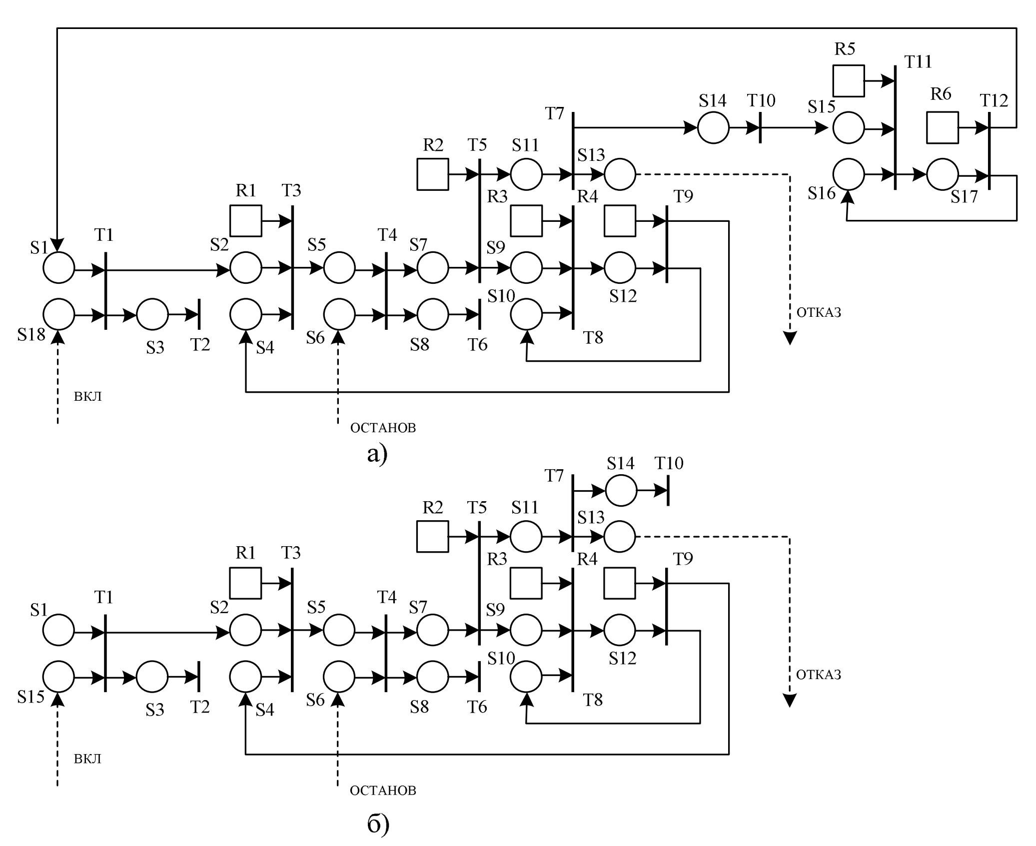


Рис. 3. Е-сети для компонента параллельной системы. Холодное резервирование: а) с восстановлением, б) без восстановления

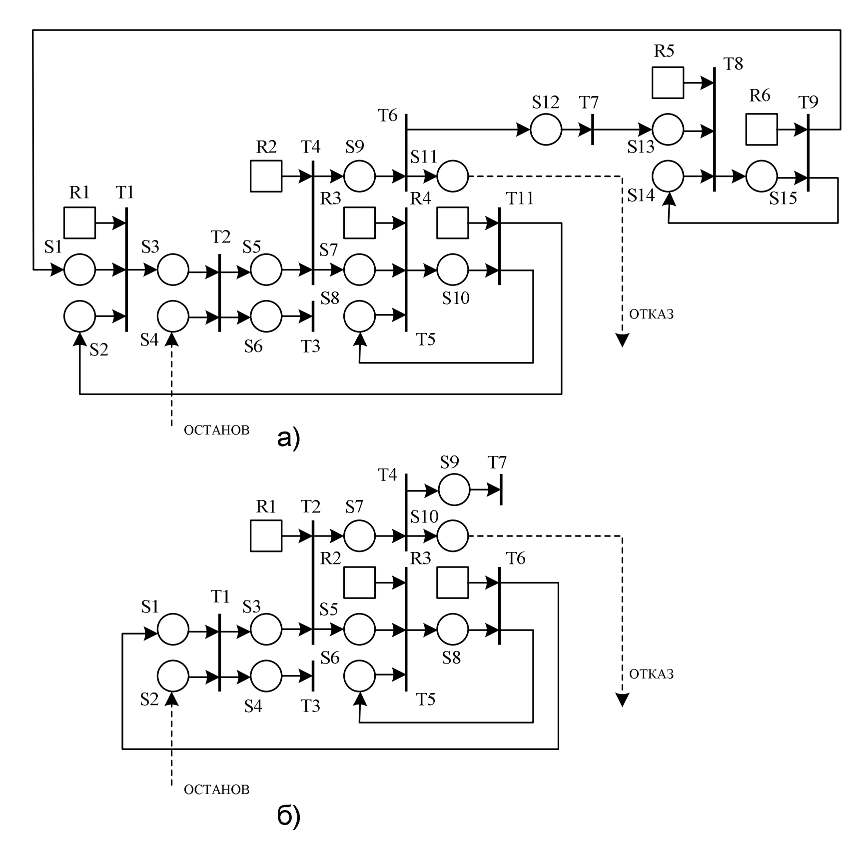


Рис. 4. Е-сети для компонента параллельной системы. Горячее резервирование: а) с восстановлением, б) без восстановления

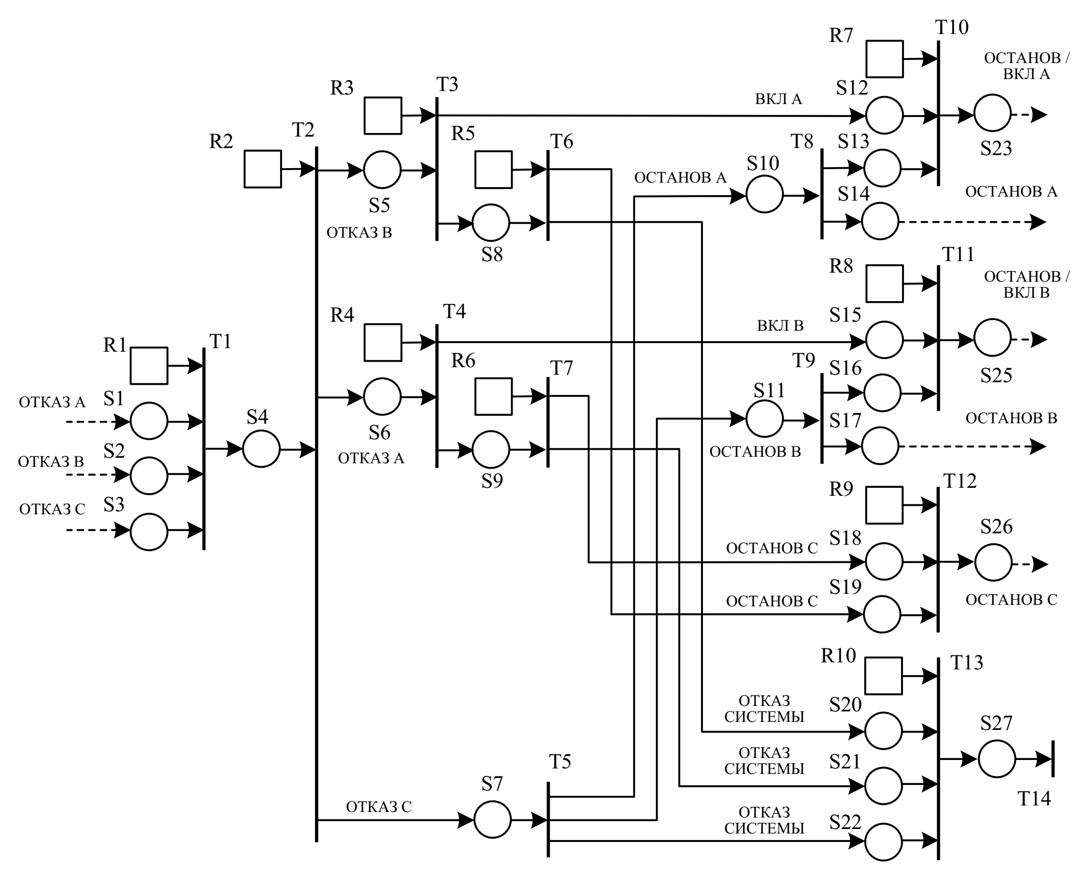


Рис. 5. *Е-сеть для управляющего устройства системы трех компонентов*

два выхода УУ: *S*10–*S*14 (останов работающего устройства *A*) и *S*10–*S*13–*S*23 (останов работы резервного устройства *A*). Такие же сигналы поступают и на компонент *B* (*S*11–*S*17 и *S*11–*S*16–*S*25).

При отказе устройства *A*, фишка проходит маршрутом *S*2–*S*4–*S*6, и далее:

- если компонент *B* работоспособен, то переключить резерв в рабочее состояние (*S*6–*S*15–*S*25);
- если компонент *B* неработоспособен, то останов устройства *C* (*S*6–*S*9–*S*18–*S*26) и отказ системы (*S*6–*S*9–*S*21–*S*27).

При отказе устройства *B* все сигналы и маршруты прохождения фишек аналогичны.

Достоинством данного подхода является возможность распространить его на случай любого количества резервных элементов, а также возможность быстро модифицировать Е-сеть для случаев нагруженного и ненагруженного резервирования с восстановлением или без восстановления. Эти модификации получаются путем удаления из Е-сети (рис. 1) позиций, переходов и дуг, упрощения разрешающих процедур и процедур преобразования атрибутов фишек, изменения сети для управляющего устройства. Подход, примененный к построению данных Е-сетей, можно использовать для построения моделей отказов-восстановлений с помощью графов или сетей более высокого уровня.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриева Е.А. Система Е-сетевого имитационного моделирования EVA. – Томск, Изд-во ТПУ, 1994. – 31 с.
2. Nutt G.J. Formulation and application of evaluation nets: PhD Thesis. – University of Washington, 1972. – 169 p.
3. Острейковский В.А. Теория надежности. – М.: Высшая школа, 2003. – 463 с.
4. Половко А.М. Основы теории надежности. – М.: Наука, 1964. – 246 с.
5. Атовмян И.О., Вайрадян А.С., Руднев Ю.П., Федосеев Ю.Н., Хетагуров Я.А. Надежность автоматизированных систем управления. – М.: Высшая школа, 1979. – 194 с.